Smart dongle

Patent number: EP1288768
Publication date: 2003-03-05
Inventor: GOTTWALD ALFRED (AT); SCHWONDRA GEORG DIPL-ING (AT)
Applicant: SIEMENS AG OESTERREICH (AT)
Classification:
- international: G06F1/00
- european:
Application number: EP20020450147 20020702
Priority number(s): AT20010001366 20010829

Also published as:
EP1288768 (A:

Cited documents:
DE10001126
EP0989497
WO02078341
EP1022638

Abstract of **EP1288768**

The method controls access to and use of a program stored in a computer which has at least one locked part. A device associated with a licensee is provided for connection to the computer. This device is adapted to unlock the locked part of the program. At least one licence message relating to the program, and at least one digital key for unlocking the locked part of the program are transmitted from the licensor to the device where they are stored in memory. When the program is started the stored message and key are tested to determine whether the locked part is to be unlocked. If so, the locked part of the program is unlocked with the digital key. Independent claims also cover an apparatus for carrying out the method.

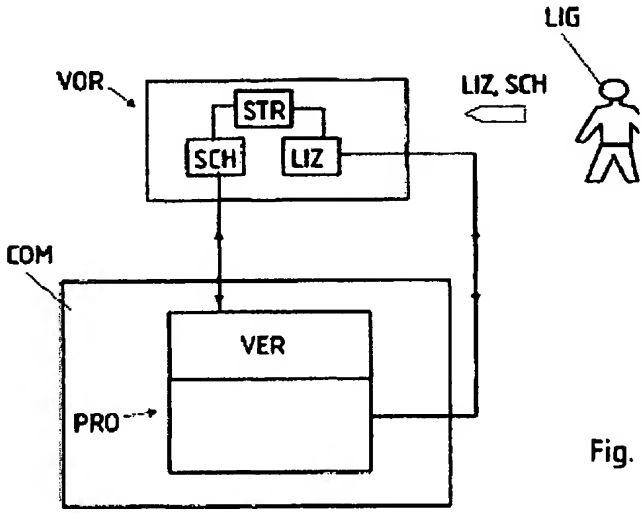

Fig.

Your Translation Results by SDL International

[0043] in accordance with fig. Another possibility of the transmission of the key SCH and/or the license message LIZ exists authorized 6 into the chip card therein, that of one of the licensor person over a petition device, for example the keyboard of the COM, that key SCH and the license message LIZ are input manually, whereby the transmission can result into the device BEFORE by means of the chip cards module or chip cards letter-/harvest device.

[0044] the license message LIZ and the key SCH can for example of the licensor LIG at a mobile phone telephone TEL of the Lizenznehmers LIG, transmitted become. This mobile phone telephone TEL shows an infrared interface ISS, the received data can become over an infrared interface of the device BEFORE at these transmitting. Alternatively in addition the Überragung of the data can surpass become of the mobile phone telephone TEL at a computer COM of the Lizenznehmers over the infrared cut yard ISS, of where out of the data transmission over a serial, parallel or USB-interface into the device BEFORE result can.

Print Page Close Window

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 288 768 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
05.03.2003 Patentblatt 2003/10

(51) Int Cl.[7]: **G06F 1/00**

(21) Anmeldenummer: **02450147.0**

(22) Anmeldetag: **02.07.2002**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **29.08.2001 AT 13662001**

(71) Anmelder: **Siemens AG Österreich**
1210 Wien (AT)

(72) Erfinder:
- **Gottwald, Alfred**
  2210 Gerasdorf (AT)
- **Schwondra, Georg , Dipl.-Ing.**
  3033 Atlengbach (AT)

(74) Vertreter: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

(54) Intelligenter Dongle

(57) Ein Verfahren und eine Vorrichtung zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf einem Computer (COM) abgelegtes Programm (PRO), welches zumindest einen verschlüsselten Teil (VER) aufweist, wobei eine mit dem Computer (COM) verbindbare einem Lizenznehmer (LIN) zugeordnete Vorrichtung (VOR) vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselten Teil (VER) des Programms (PRO) zu entschlüsseln, wobei zumindest eine das Programm (PRO) betreffende Lizenznachricht (LIZ) und zumindest ein digitalen Schlüssel (SCH) zum Entschlüsseln des verschlüsselten Teils (VER) des Programms (PRO) von einem Lizenzgeber (LIG) an die Vorrichtung (VOR) übertragen werden, wo diese in einem Speicher abgelegt werden und auf Anforderung anhand der abgelegten Lizenznachricht (LIZ) überprüft wird, ob der verschlüsselte Teil (VER) des Programms (PRO) zu entschlüsseln ist und abhängig vom Ergebnis dieser Überprüfung der verschlüsselte Teil (VER) mithilfe des abgelegten, digitalen Schlüssels (SCH) entschlüsselt wird.

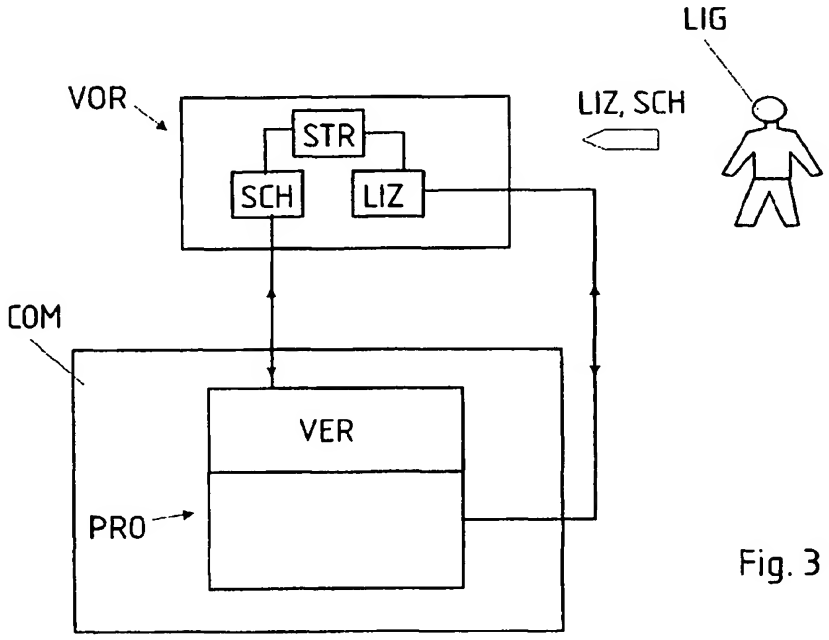

Fig. 3

EP 1 288 768 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf einem Computer abgelegtes Programm, welches zumindest einen verschlüsselten Teil aufweist, wobei eine mit dem Computer verbindbare, einem Lizenznehmer zugeordnete Vorrichtung vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselten Teil des Programms zu entschlüsseln.

[0002] Weiters betrifft die Erfindung eine mit einem Computer verbindbare, einem Lizenznehmer zugeordnete Vorrichtung zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf dem Computer abgelegtes Programm, welches zumindest einen verschlüsselten Teil aufweist, wobei eine Steuerung vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselte Teil des Programms zu entschlüsseln.

[0003] Vorrichtungen und Verfahren der oben genannten Art sind unter der Bezeichnung "Dongle" bekannt geworden. Bei einem Dongle handelt es sich um eine hardwarebasierte Sicherheitsvorrichtung, die beispielsweise an einen seriellen oder parallelen Druckerport eines Desktop-Computers oder einen Kartensteckplatz eines Laptops anbindbar ist. Ein Schlüssel zum entschlüsseln verschlüsselter Programmteile und beispielsweise Passwörter sind bekannterweise hardcodiert in den herkömmlichen Dongles abgelegt. D. h. im Rahmen der Herstellung wird ein Schlüssel zur Entschlüsselung verschlüsselter Teile eines vorgebbaren Programms bzw. Lizenzinformationen fix in den Dongle implementiert. Eine nachträgliche Erweiterung um andere Schlüssel für andere Programme bzw. Änderungen von Nutzungsbedingungen oder -berechtigungen ist nicht in gesicherter Form möglich. Nachteilig an dieser Methode ist, dass für jedes Programm, welches mittels verschlüsselter Teile vor einer unbefugten Benutzung geschützt ist, ein eigener Dongle hergestellt werden muss, auch können die voreingestellten, hardcodierten Nutzungsbedingungen bei den bekannten Vorrichtungen nicht geändert werden.

[0004] Es ist daher eine Aufgabe der Erfindung, einen Weg zu schaffen, der die oben genannten Nachteile überwindet.

[0005] Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art erfindungsgemäß dadurch gelöst, dass zumindest eine das Programm betreffende Lizenznachricht und zumindest ein digitaler Schlüssel zum Entschlüsseln des verschlüsselten Teils des Programms von einem Lizenzgeber an die Vorrichtung übertragen werden, wo der Schlüssel und die Lizenznachricht in einem Speicher abgelegt werden, und bei Starten des Programms anhand der abgelegten Lizenznachricht überprüft wird, ob der verschlüsselte Teil des Programms zu entschlüsseln ist, und abhängig von dem Ergebnis dieser Überprüfung der verschlüsselte Teil mithilfe des abgelegten, digitalen Schlüssels entschlüsselt wird.

[0006] Diese Lösung ermöglicht es im Gegensatz zu den bekannten hardcodierten Dongles nachträglich Änderungen der Nutzungsbedingungen durchzuführen bzw. die Vorrichtung um neue Schlüssel zu erweitern, sodass sie problemlos an beliebige Programme angepasst werden können. Die Erfindung erlaubt somit auch die Realisierung eines "Dongles" der für mehrere Programme, die mit unterschiedlichen Schlüsseln zu entschlüsseln sind, verwendet werden kann. Im Prinzip können mit der erfindungsgemäßen Lösung beliebig viele Schlüssel und Lizenzinformationen, d. h. Nutzungsbedingungen etc., in einem Dongle realisiert werden, wobei diese Daten an geänderte Nutzungsbedingungen angepasst werden können.

[0007] Um eine sichere Übertragung des Schlüssel und der Lizenzinformationen zu gewährleisten, können die zumindest eine Lizenznachricht und der digitale Schlüssel in verschlüsselter Form an die Vorrichtung übertragen und von einer Steuerung der Vorrichtung entschlüsselt und in entschlüsselter Form in dem Speicher abgelegt werden.

[0008] Zusätzlich kann die Lizenznachricht Zahlungsdaten betreffend die Zahlungsart bzw. die Zahlungsmodalitäten enthalten.

[0009] Eine vorteilhafte Variante der Erfindung sieht vor, dass die Lizenznachricht Zeitdaten, betreffend die Gültigkeitsdauer eines Benutzungszeitraumes für das Programm, enthält.

[0010] Weiters kann die Vorrichtung anhand einer Signatur des Programms dessen Authentizität überprüfen.

[0011] Eine bevorzugte Ausführungsform der Erfindung sieht vor, dass der Schlüssel und die Lizenznachricht zumindest abschnittsweise über ein Datennetz übertragen werden.

[0012] Eine andere Möglichkeit, den Schlüssel und die Lizenznachricht zu übertragen, besteht darin, dass der Schlüssel und die Lizenznachricht zumindest abschnittsweise über ein Funknetz übertragen werden.

[0013] Darüber hinaus können der Schlüssel und die Lizenznachricht auch über eine mit der Vorrichtung verbundene Eingabevorrichtung manuell eingegeben werden.

[0014] Weitere Vorteile lassen sich dadurch erzielen, dass die Lizenznachricht zumindest einen Freischaltcode für zumindest ein noch nicht freigeschaltetes Leistungsmerkmal bzw. einen noch nicht freigeschalteten verschlüsselten Teil des Programms enthält.

[0015] Weitere Vorteile lassen sich dadurch erzielen, dass die Vorrichtung als Chipkarte ausgeführt ist und der Schlüssel und die Lizenznachricht über ein mit einem Computer verbundenes Chipkartenmodul oder ein Chipkartenschreibgerät an die Vorrichtung übertragen werden.

[0016] Weitere Vorteile lassen sich dadurch erzielen, dass ein Datenaustausch zwischen der Vorrichtung und dem Programm über ein Chipkartenmodul oder ein Chipkartenlesegerät erfolgt.

DOCID: <EP___1288768A2_I_>

[0017] Zur Durchführung des erfindungsgemäßen Verfahren eignet sich insbesondere eine Vorrichtung der eingangs genannten Art, welche eine Ein/Ausgabeeinheit aufweist, welche dazu eingerichtet ist, von einem einem Lizenzgeber zugeordneten Telekommunikationsendgerät eine das Programm betreffende Lizenznachricht und zumindest einen digitalen Schlüssel zum Entschlüsseln des verschlüsselten Teils des Programms, zu empfangen und an die Steuerung weiterzuleiten, die dazu eingerichtet ist den digitalen Schlüssel und die Lizenznachricht in einem Speicher abzulegen und bei Starten des Programms anhand der Lizenznachricht zu überprüfen, ob der verschlüsselten Teil des Programms zu entschlüsseln ist und abhängig vom Ergebnis dieser Überprüfung den verschlüsselten Teil mithilfe des digitalen Schlüssels zu entschlüsseln.

[0018] Vorteilhafterweise kann die Lizenznachricht Zahlungsdaten betreffend die Zahlungsart enthalten.

[0019] Weitere Vorteile lassen sich dadurch erzielen, dass die Lizenznachricht Zeitdaten betreffend die Gültigkeitsdauer eines Benutzungszeitraumes für das Programm enthält.

[0020] Darüber hinaus kann die Vorrichtung dazu eingerichtet sein, anhand einer Signatur des Programms dessen Authentizität zu überprüfen.

[0021] Eine bevorzugte Ausführungsform der Erfindung sieht vor, dass sie als Chipkarte ausgeführt ist und über ein Chipkartenmodul oder ein Lesegerät an den Computer anbindbar ist.

[0022] Eine andere, günstige Variante der Erfindung besteht darin, dass die Vorrichtung mit einer Eingabevorrichtung verbindbar ist, die dazu eingerichtet ist den Schlüssel und die Lizenznachricht über ein Datennetz zu empfangen.

[0023] In einer weiteren Variante der Erfindung kann die Vorrichtung mit einer Eingabevorrichtung verbindbar sein, die dazu eingerichtet ist, den Schlüssel und die Lizenznachricht über ein Funknetz zu empfangen.

[0024] Eine weitere sehr vorteilhafte Variante der Erfindung sieht vor, dass die Vorrichtung mit einer Eingabevorrichtung verbindbar ist, über welche der Schlüssel und Lizenznachricht manuell eingebbar sind.

[0025] Die Lizenznachricht kann zumindest einen Freischaltcode für zumindest ein noch nicht freigeschaltetes Leistungsmerkmal bzw. einen noch nicht freigeschalteten, verschlüsselten Teil des Programms enthalten.

[0026] Weiters kann die Vorrichtung dazu eingerichtet sein, die zumindest eine Lizenznachricht und den digitale Schlüssel in verschlüsselter Form zu empfangen und die Steuerung kann dazu eingerichtet sein, die Lizenznachricht und den Schlüssel zu entschlüsseln und in entschlüsselter Form in dem Speicher abzulegen.

[0027] In einer bevorzugten Ausführungsform der Erfindung ist die Vorrichtung als Chipkarte ausgeführt und der Schlüssel und die Lizenznachricht über ein mit einem Computer verbundenes Chipkartenmodul oder ein Chipkartenschreibgerät an die Vorrichtung übertragen werden.

[0028] Weiters kann die Eingabe/Ausgabeeinheit dazu eingerichtet sein, über ein Chipkartenmodul oder ein Chipkartenlesegerät mit dem Programm Daten auszutauschen.

[0029] Die Erfindung samt weiteren Vorteilen wird im folgenden anhand einiger nicht einschränkender Ausführungsbeispiele näher erläutert, die in der Zeichnung dargestellt sind, in dieser zeigen schematisch:

Fig. 1 eine erfindungsgemäße Vorrichtung;

Fig. 2 eine Übertragung einer Lizenznachricht und eines digitalen Schlüssels in eine erfindungsgemäße Vorrichtung;

Fig. 3 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens;

Fig. 4 eine erfindungsgemäße Lizenznachricht;

Fig. 5 eine erfindungsgemäße Speichereinheit;

Fig. 6 eine Übertragungsart der Lizenznachricht und des digitalen Schlüssels aus Fig. 2 in die erfindungsgemäße Vorrichtung aus Fig. 1;

Fig. 7 eine weitere Übertragungsart der Lizenznachricht und des digitalen Schlüssels in die erfindungsgemäße Vorrichtung aus Fig. 1 und

Fig. 8 die Verwendung der erfindungsgemäßen Vorrichtung aus Fig. 1 in einem Netzwerk.

[0030] Gemäß Fig. 1 weist eine erfindungsgemäße Vorrichtung eine Eingabe/Ausgabeeinheit EAE auf mit der es Daten mit einem Computer COM bzw. mit einem auf diesem abgelegtem Programm, welches verschlüsselte Programmteile aufweist austauschen kann. Die Eingabe/Ausgabeeinheit EAE steht mit einer Steuerung STR in Verbindung, die auf den Inhalt eines Speichers STR zugreifen kann, um die Entschlüsselung verschlüsselter Teile des Programms durchzuführen. Erst die Entschlüsselung der verschlüsselten Teile macht diese für einen Benutzer anwendbar. In einer bevorzugten Ausführungsform der Erfindung ist die Vorrichtung VOR als Chipkarte ausgeführt. Verfügt der Computer COM über eine USB-Schnittstelle so kann die Anbindung der Chipkarte an den Computer über ein Chipkartenmodul CMO erfolgen. Weist der Computer COM nur eine parallele oder serielle Schnittstelle auf, so kann die Anbindung der Chipkarte an den Computer COM über ein Chipkartenlesegerät LES (FIG. 2) erfolgen.

[0031] Nach Fig. 2 kann die Übertragung eines von der Steuerung STR benötigten Schlüssels SCH und von Lizenzinformationen LIZ, welche Nutzungsbedingungen für das Programm bzw. für die verschlüsselten Programmteile vorgeben, beispielsweise von einem Server

SER eines Lizenzgebers LIG an den mit der erfindungsgemäßen Vorrichtung VOR verbundnen Computer COM übertragen werden. Die an den Computer COM übertragenen Informationen können, beispielsweise über eine serielle, parallele oder USB-Schnittstelle in die Vorrichtung VOR übertragen werden. In einer bevorzugten Ausführungsform der Erfindung ist die Vorrichtung VOR als Chipkarte realisiert, die über ein Chipkartenmodul oder ein Chipkartenlesegerät an den Computer COM angebunden werden kann.

[0032] Gemäß Fig. 3 überprüft die Steuerung STR der Vorrichtung VOR, wenn ein Benutzer das Programm PRO starten möchte, anhand der von einem Lizenzgeber LIG an die Vorrichtung VOR übermittelten, in dem Speicher SPR abgelegten Lizenzinformationen LIZ, ob eine Entschlüsselung der verschlüsselten Teile VER des Programms PRO mittels des Schlüssels SCH erfolgen soll. Ergibt diese Überprüfung, dass für eine aktuelle Benutzung des Programms bzw. der verschlüsselten Programmteile eine Lizenz vorhanden ist, so wird die Entschlüsselung des verschlüsselten Programmteiles durchgeführt, wobei das Programm PRO so realisiert sein kann, dass es ohne Entschlüsselung des verschlüsselten Teiles nicht oder nur eingeschränkt benutzbar ist. Ergibt die Überprüfung der Lizenzinformationen, dass für die Benutzung des Programms PRO bzw. des verschlüsselten Teils VER keine Lizenz vorhanden ist, so wird der verschlüsselte Teil VER des Programms PRO nicht entschlüsselt, sodass eine Benutzung des Programms PRO nicht oder nur eingeschränkt möglich ist.

[0033] Darüber hinaus kann die Vorrichtung dazu eingerichtet sein, anhand einer Signatur des Programms dessen Authentizität zu überprüfen. Auf diese Weise kann sichergestellt werden, dass es sich bei dem benutzten Programm PRO um eine authentische und unmanipulierte Version des Programms PRO handelt. Auch kann dadurch erkannt werden, wenn eine andere Version des Programms PRO installiert wird.

[0034] Nach Fig. 4 kann die Lizenznachricht LIZ eine Headernachricht enthalten, anhand welcher die Steuerung STR erkennen kann, dass es sich um eine Lizenznachricht LIZ handelt. Weiters kann die Lizenznachricht beispielsweise Zahlungsdaten ZAD, betreffend die Zahlungsart der Nutzungsberechtigung, "Application Identification" Daten API zur Identifizierung des Programms PRO, sowie Zeitdaten DAU, betreffend die Gültigkeitsdauer der Nutzungsberechtigung, enthalten.

[0035] Mögliche Zahlungsarten bzw. Modalitäten wären z. B. eine online Zahlung bei Programmstart, in diesem Fall kann, vorausgesetzt es besteht eine Kommunikationsverbindung zwischen der Vorrichtung VOR und einem Telekommunikationsendgerät SER, SEN des Lizenzgebers LIG, eine Abbuchung von einem vorher bekanntgegebenen Konto des Lizenznehmers erfolgen. Eine andere Zahlungsart besteht beispielsweise darin, dass die Benutzungsdauer erfasst und in der Vorrichtung oder dem Computer COM gespeichert wird und zu einem späteren Zeitpunkt mit dem Lizenzgeber abgerechnet wird. Prinzipiell sind natürlich beliebige Zahlungsarten möglich.

[0036] Bei Programmstart identifiziert sich das Programm PRO gegenüber der Vorrichtung VOR. Anhand der Daten API zur Identifizierung des Programms PRO kann die Steuerung STR das Programm PRO erkennen. Wird das Programm von der Steuerung STR erfolgreich identifiziert so überprüft die Steuerung STR, ob bzw. in welchem Umfang Nutzungsberechtigungen für das Programm PRO vorliegen.

[0037] Natürlich kann die Lizenznachricht LIZ noch andere Daten betreffend die Nutzungsbedingungen und Nutzungsrechte enthalten. So können beispielsweise Freischaltcodes COD für noch nicht aktivierte Features des Programms PRO ebenfalls in der Lizenznachricht enthalten sein.

[0038] Besteht eine Nutzungsberechtigung für eine vorgebbare Anzahl von Benutzungen des Programms so kann bei jedem Programmstart ein Nutzungszähler inkrementiert oder dekrementiert werden, wobei entweder bei erreichen der höchsten eingestellten Nutzungszahl oder des Wertes Null eine weitere Nutzung des Programms nicht mehr möglich ist, da in diesem Fall eine Entschlüsselung der verschlüsselten Programmteile seitens der Steuerung STR nicht mehr erfolgt.

[0039] Bei den in der Lizenznachricht enthaltenen Daten kann es sich aber auch um Zeitdaten handeln, die zur Benutzung des Programms in einem vorgebbaren Zeitraum berechtigt.

[0040] Gemäß Fig. 5 können in der Lizenznachricht LIZ enthaltenen Daten in Form beispielsweise in Form einer Tabelle TAB in dem Speicher SPR abgelegt sein. Dabei kann mehreren ein Programm PRO, PR1, PR2, PR3 betreffende Lizenzinformationen ein Schlüssel SCH, SC1, SC2 zugeordnet sein. Natürlich können auch einem Programm PRO, PR1, PR2, PR3 mehrere Schlüssel SCH zugeordnet sein, die unterschiedlich verschlüsselte Programmteile eines Programms entschlüsseln können. Erwirbt ein Benutzer beispielsweise, die Lizenz zur Benutzung einer Grundversion des Programms PRO, so kann das Programm PRO trotz allem in der Vollversion auf dem Computer COM des Lizenznehmers LIN installiert werden, wobei die erweiterten Leistungsmerkmale und Programmteile verschlüsselt bleiben. Sind verschiedene Programmteile diese Programms unterschiedlich verschlüsselt, so muss zum Freischalten eines dieser Programmteile der dazupassende Schlüssel erworben werden, sodass für ein Programm auch mehrere Schlüssel vorgesehen sein können.

[0041] Anhand der Lizenzinformationen kann, wie bereits oben erwähnt, von der Steuerung STR entschieden werden, welche der verschlüsselten Programmteile entschlüsselt werden dürfen. Erweitert der Lizenznehmer LIN durch Kauf einer weiteren Nutzungsberechtigung seine Nutzungsbefugnis, so können, falls die verschlüsselten Teile nach der gleichen Methode ver-

schlüsselt sind, auch mit dem selben Schlüssel SCH weitere Programmteile entschlüsselt werden.

[0042] Nach Fig. 6 können der Schlüssel SCH und die Lizenznachricht LIZ, welche die von einem Lizenznehmer gewünschte Art des Nutzungsumfanges und der Nutzungsbedingungen enthält, über ein Datennetz DAT, beispielsweise das Internet, an die Vorrichtung VOR übertragen werden. Ist die Vorrichtung VOR als Chipkarte ausgeführt, so kann sie, wie bereits oben erwähnt, mittels eines Chipkartenmoduls bzw. -lesegeräts an einen Computer COM angeschlossen sein. Ist dieser Computer COM dem Datennetz DAT, z. B. dem Internet verbunden, so kann die Übertragung der Lizenznachricht LIZ an den Computer COM, beispielsweise gemäß dem TCP/IP - Protokoll, erfolgen. Die von dem Computer COM erhaltenen Daten können dann über das Chipkartenmodul oder -schreib/Lesegerät in die Chipkarte übertragen werden.

[0043] Gemäß Fig. 6 besteht eine andere Möglichkeit der Übertragung des Schlüssels SCH bzw. der Lizenznachricht LIZ in die Chipkarte darin, dass von einer von dem Lizenzgeber autorisierten Person über eine Eingabevorrichtung, beispielsweise die Tastatur des COM, der Schlüssel SCH und die Lizenznachricht LIZ manuell eingegeben werden, wobei die Übertragung in die Vorrichtung VOR mittels des Chipkartenmoduls oder Chipkartenschreib-/Lesegeräts erfolgen kann.

[0044] Die Lizenznachricht LIZ und der Schlüssel SCH können beispielsweise von dem Lizenzgeber LIG an ein Mobilfunktelefon TEL des Lizenznehmers LIG, übermittelt werden. Weist dieses Mobilfunktelefon TEL eine Infrarotschnittstelle ISS auf, so können die empfangenen Daten über eine Infrarotschnittstelle der Vorrichtung VOR an diese Übertragen werden. Alternativ dazu kann die Überragung der Daten von dem Mobilfunktelefon TEL an einen Computer COM des Lizenznehmers über die Infrarotschnittselle ISS überragen werden, von wo aus die Datenübertragung über eine serielle, parallele oder USB-Schnittstelle in die Vorrichtung VOR erfolgen kann.

[0045] Nach Fig. 8 können die in der Vorrichtung abgelegten Nutzungsrechte und Schlüssel in einem Netzwerk NET, beispielsweise von einem Verwaltungsserver VSE, zentral verwaltet werden. Hat eine Firma beispielsweise ein Lizenzpaket zur Benutzung eines Programms für hundert Mitarbeiter erworben, so können diese Lizenzen von dem Verwaltungsserver über das Netzwerk NET an die Vorrichtungen VOR übertragen und im Bedarfsfall wieder entzogen, d.h. aus dem Speicher der Vorrichtung VOR gelöscht werden. Die Realisierungsmöglichkeit der erfindungsgemäßen Vorrichtung als Chipkarte ermöglicht einem Benutzer darüber hinaus, sich an jedem beliebigen Computer COM des Netzwerkes zu begeben und dort die für ihn freigeschalteten Programme zu benutzen.

Patentansprüche

1. Verfahren zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf einem Computer (COM) abgelegtes Programm (PRO), welches zumindest einen verschlüsselten Teil (VER) aufweist, wobei eine mit dem Computer (COM) verbindbare, einem Lizenznehmer (LIN) zugeordnete Vorrichtung (VOR) vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselten Teil (VER) des Programms (PRO) zu entschlüsseln, **dadurch gekennzeichnet, dass** zumindest eine das Programm (PRO) betreffende Lizenznachricht (LIZ) und zumindest ein digitaler Schlüssel (SCH) zum Entschlüsseln des verschlüsselten Teils (VER) des Programms (PRO) von einem Lizenzgeber (LIG) an die Vorrichtung (VOR) übertragen werden, wo der Schlüssel (SCH) und die Lizenznachricht (LIZ) in einem Speicher (SPR) abgelegt werden, und bei Starten des Programms (PRO) anhand der abgelegten Lizenznachricht (LIZ) überprüft wird, ob der verschlüsselte Teil (VER) des Programms (PRO) zu entschlüsseln ist, und abhängig von dem Ergebnis dieser Überprüfung der verschlüsselte Teil (VER) mithilfe des abgelegten, digitalen Schlüssels (SCH) entschlüsselt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die zumindest eine Lizenznachricht (LIZ) und der digitale Schlüssel (SCH, SC1, SC2, SC3) in verschlüsselter Form an die Vorrichtung (VOR) übertragen und von einer Steuerung (STR) der Vorrichtung (VOR) entschlüsselt und in entschlüsselter Form in dem Speicher (SPR) abgelegt werden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) Zahlungsdaten (ZAD, ZA1, ZA2, ZA3) betreffend die Zahlungsart enthält.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) Zeitdaten (ZEI, ZE1, ZE2, ZE3) betreffend die Gültigkeitsdauer eines Benutzungszeitraumes für das Programm (PRO, PR1, PR2, PR3) enthält.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** die Vorrichtung anhand einer Signatur des Programms (PRO) dessen Authentizität überprüft.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** der Schlüssel (SCH) und die Lizenznachricht (LIZ) zumindest abschnittsweise über ein Datennetz (DAT) übertragen werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** der Schlüssel (SCH) und die Lizenznachricht (LIZ) zumindest abschnittsweise über ein Funknetz (FUN) übertragen werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** der Schlüssel (SCH) und die Lizenznachricht (LIZ) über eine mit der Vorrichtung (VOR) verbundene Eingabevorrichtung manuell eingegeben werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) zumindest einen Freischaltcode (COD) für zumindest ein noch nicht freigeschaltetes Leistungsmerkmal bzw. einen noch nicht freigeschalteten verschlüsselten Teil (VER) des Programms (PRO) enthält.

10. Verfahren nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** die Vorrichtung (VOR) als Chipkarte ausgeführt ist und der Schlüssel (SCH) und die Lizenznachricht (LIZ) über ein mit dem Computer (COM) verbundenes Chipkartenmodul oder ein Chipkartenschreibgerät an die Vorrichtung übertragen werden.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet, dass** ein Datenaustausch zwischen der Vorrichtung (VOR) und dem Programm (PRO) über ein Chipkartenmodul oder ein Chipkartenlesegerät erfolgt.

12. Mit einem Computer (COM) verbindbare, einem Lizenznehmer (LIZ) zugeordnete Vorrichtung (VOR) zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf dem Computer (COM) abgelegtes Programm (PRO), welches zumindest einen verschlüsselten Teil (VER) aufweist, wobei eine Steuerung (STR) vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselte Teil (VER) des Programms (PRO) zu entschlüsseln, **dadurch gekennzeichnet, dass** sie eine Ein/Ausgabeeinheit (EAE) aufweist, welche dazu eingerichtet ist, von einem einem Lizenzgeber (LIG) zugeordnetem Telekommunikationsendgerät (SER, SEN) eine das Programm (PRO) betreffende Lizenznachricht (LIZ) und zumindest einen digitalen Schlüssel (SCH) zum Entschlüsseln des verschlüsselten Teils (VER) des Programms (PRO) zu empfangen und an die Steuerung (STR) weiterzuleiten, die dazu eingerichtet ist, den digitalen Schlüssel (SCH) und die Lizenznachricht (LIZ) in einem Speicher (SPR) abzulegen und bei Starten des Programms (PRO) anhand der Lizenznachricht (LIZ) zu überprüfen, ob der verschlüsselten Teil (VER) des Programms (PRO) zu entschlüsseln ist, und abhängig vom Ergebnis dieser Überprüfung den verschlüsselten Teil (VER) mithilfe des digitalen Schlüssels (SCH) zu entschlüsseln.

13. Vorrichtung nach Anspruch 12, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) Zahlungsdaten (ZAL) betreffend die Zahlungsart enthält.

14. Vorrichtung nach Anspruch 12 oder 13, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) Zeitdaten (ZEI) betreffend die Gültigkeitsdauer eines Benutzungszeitraumes für das Programm (PRO) enthält.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, **dadurch gekennzeichnet, dass** sie dazu eingerichtet ist, anhand einer Signatur des Programms (PRO) dessen Authentizität zu überprüfen.

16. Vorrichtung nach einem der Ansprüche 12 bis 15, **dadurch gekennzeichnet, dass** sie als Chipkarte ausgeführt ist und über ein Chipkartenmodul oder ein Lesegerät an den Computer (COM) anbindbar ist.

17. Vorrichtung nach einem der Ansprüche 12 bis 16, **dadurch gekennzeichnet, dass** sie mit einer Eingabevorrichtung verbindbar ist, die dazu eingerichtet ist, den Schlüssel (SCH) und die Lizenznachricht (LIZ) über ein Datennetz (DAT) zu empfangen.

18. Vorrichtung nach einem der Ansprüche 12 bis 17, **dadurch gekennzeichnet, dass** sie mit einer Eingabevorrichtung verbindbar ist, die dazu eingerichtet ist den Schlüssel (SCH) und die Lizenznachricht (LIZ) über ein Funknetz (FUN) zu empfangen.

19. Vorrichtung nach einem der Ansprüche 12 bis 18, **dadurch gekennzeichnet, dass** sie mit einer Eingabevorrichtung verbindbar ist, über welche der Schlüssel (SCH) und die Lizenznachricht (LIZ) manuell eingebbar sind.

20. Vorrichtung nach einem der Ansprüche 12 bis 19, **dadurch gekennzeichnet, dass** die Lizenznachricht (LIZ) zumindest einen Freischaltcode (COD) für zumindest ein noch nicht freigeschaltetes Leistungsmerkmal bzw. einen noch nicht freigeschalteten, verschlüsselten Teil (VER) des Programms enthält.

21. Vorrichtung nach einem der Ansprüche 12 bis 20, **dadurch gekennzeichnet, dass** sie dazu eingerichtet ist, die zumindest eine Lizenznachricht (LIZ) und den digitalen Schlüssel (SCH) in verschlüsselter Form zu empfangen, und die Steuerung (STR) dazu eingerichtet ist, die Lizenznachricht (LIZ) und den Schlüssel (SCH) zu entschlüsseln und in ent-

schlüsselter Form in dem Speicher (SPR) abzulegen.

22. Vorrichtung nach einem der Ansprüche 12 bis 21, **dadurch gekennzeichnet, dass** die Vorrichtung (VOR) als Chipkarte ausgeführt ist und der Schlüssel (SCH) und die Lizenznachricht (LIZ) über ein mit dem Computer (COM) verbundenes Chipkartenmodul oder ein Chipkartenschreibgerät an die Vorrichtung (VOR) übertragen werden.

23. Vorrichtung nach einem der Ansprüche 12 bis 22 **dadurch gekennzeichnet, dass** die Eingabe/Ausgabeeinheit (EAE) dazu eingerichtet ist, über ein Chipkartenmodul oder ein Chipkartenlesegerät mit dem Programm (PRO) Daten auszutauschen.

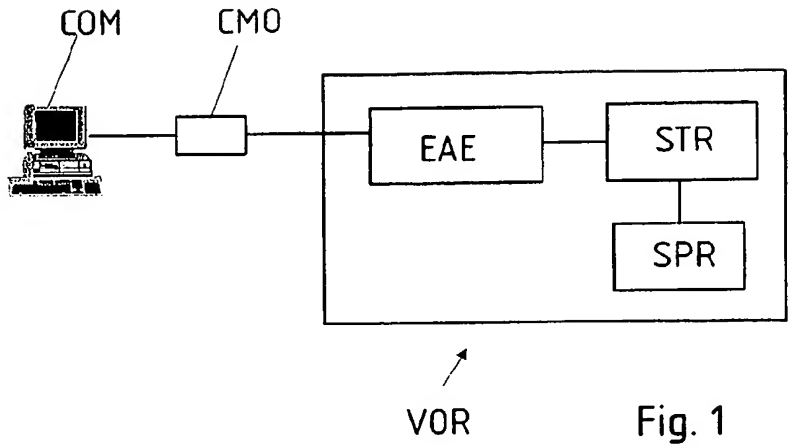

Fig. 1

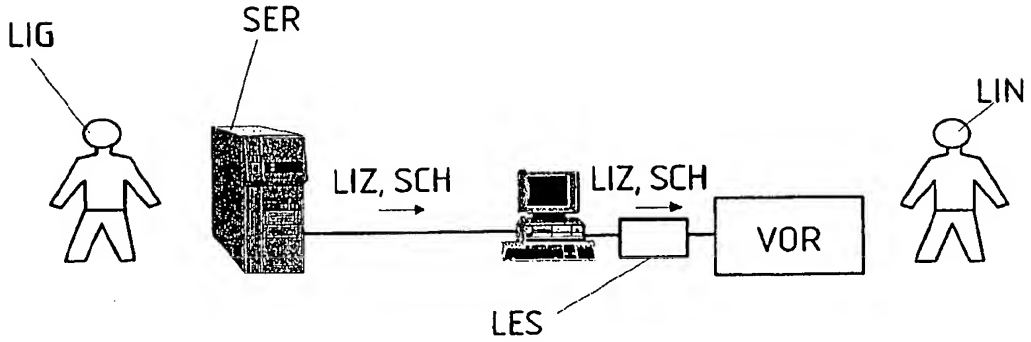

Fig. 2

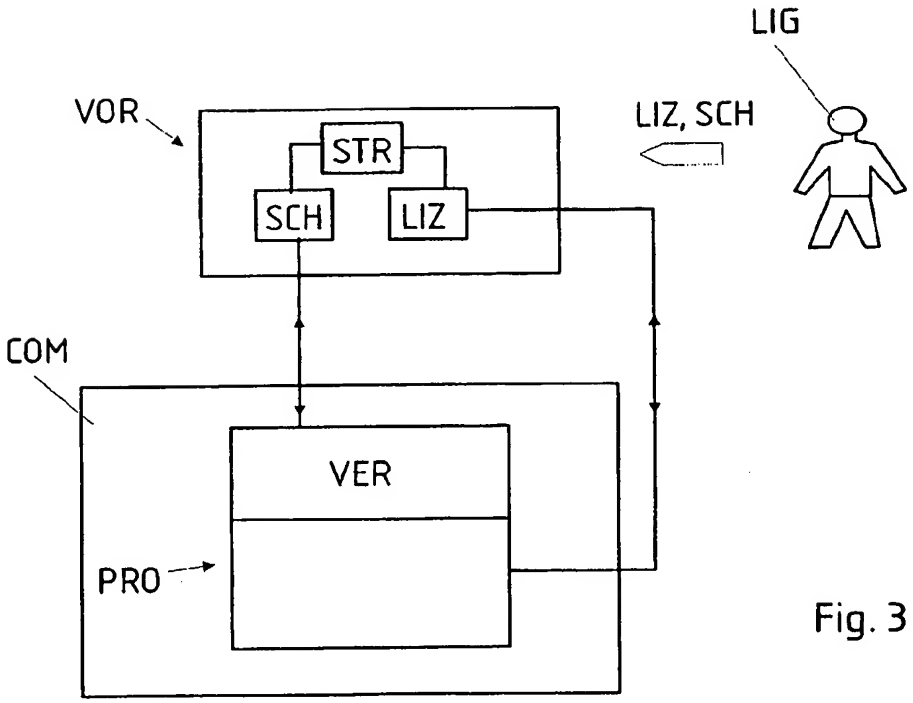

Fig. 3

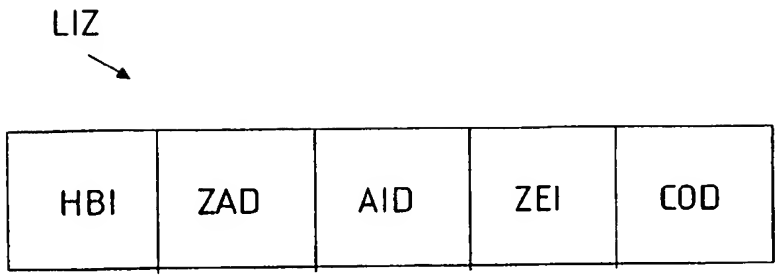

Fig. 4

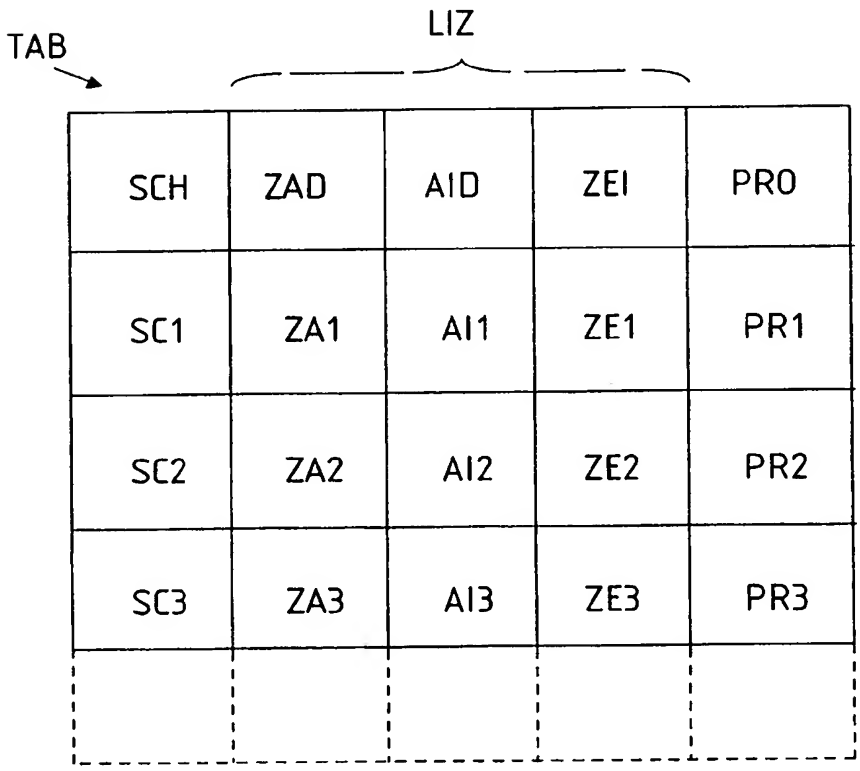

Fig. 5

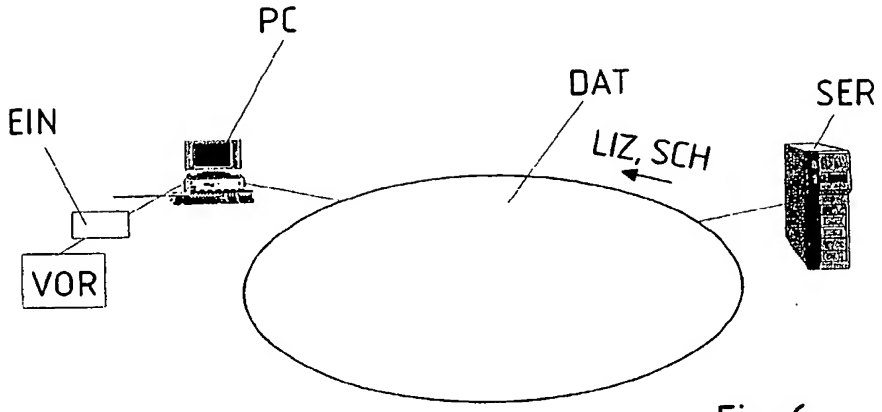

Fig. 6

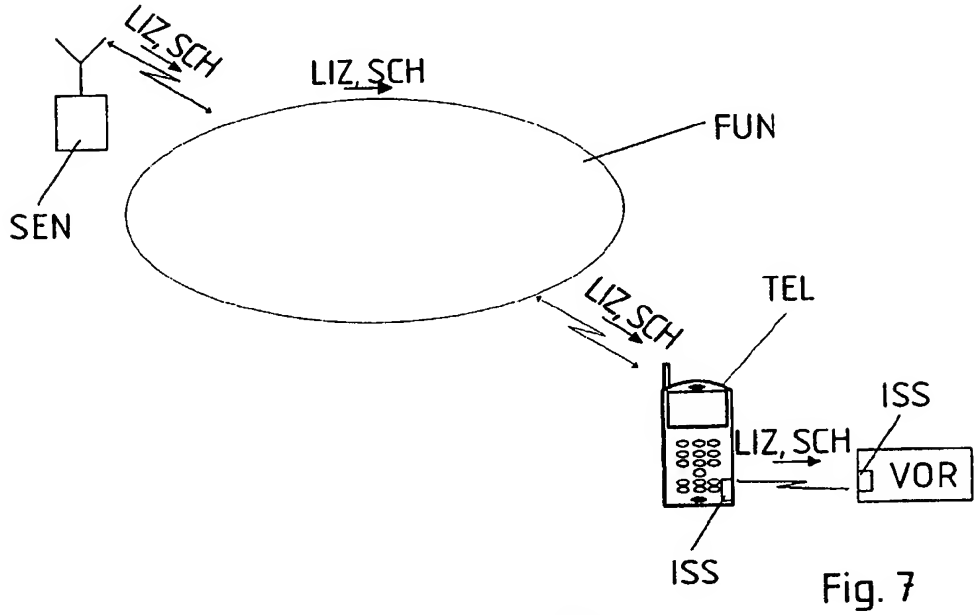

Fig. 7

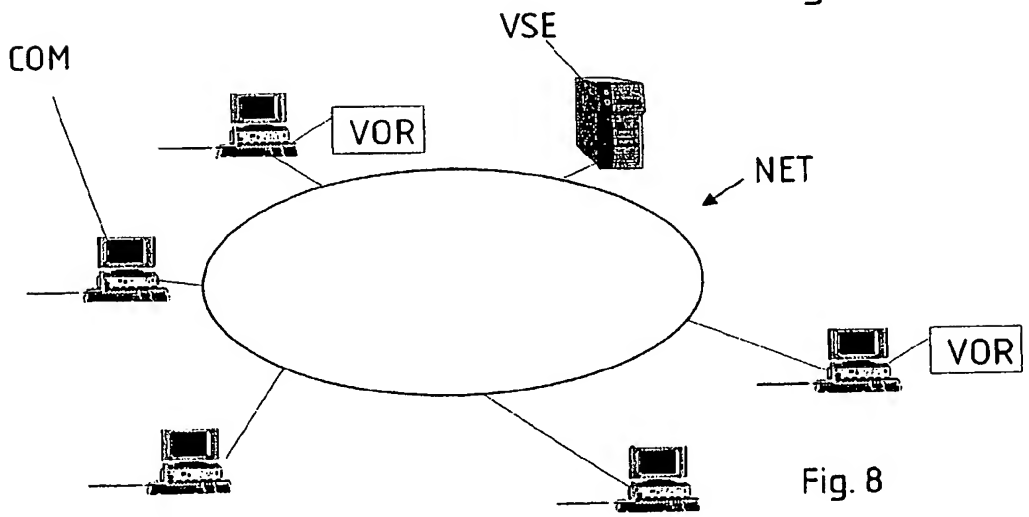

Fig. 8

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 288 768 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
02.01.2004 Patentblatt 2004/01

(43) Veröffentlichungstag A2:
05.03.2003 Patentblatt 2003/10

(21) Anmeldenummer: **02450147.0**

(22) Anmeldetag: **02.07.2002**

(51) Int Cl.[7]: **G06F 1/00**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **29.08.2001 AT 13662001**

(71) Anmelder: **Siemens AG Österreich**
1210 Wien (AT)

(72) Erfinder:
- **Gottwald, Alfred**
  2210 Gerasdorf (AT)
- **Schwondra, Georg , Dipl.-Ing.**
  3033 Atlengbach (AT)

(74) Vertreter: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

(54) Intelligenter Dongle

(57) Ein Verfahren und eine Vorrichtung zur sicheren Zugangs/Benutzungskontrolle für zumindest ein auf einem Computer (COM) abgelegtes Programm (PRO), welches zumindest einen verschlüsselten Teil (VER) aufweist, wobei eine mit dem Computer (COM) verbindbare einem Lizenznehmer (LIN) zugeordnete Vorrichtung (VOR) vorgesehen ist, die dazu eingerichtet ist, den zumindest einen verschlüsselten Teil (VER) des Programms (PRO) zu entschlüsseln, wobei zumindest eine das Programm (PRO) betreffende Lizenznachricht (LIZ) und zumindest ein digitalen Schlüssel (SCH) zum Entschlüsseln des verschlüsselten Teils (VER) des Programms (PRO) von einem Lizenzgeber (LIG) an die Vorrichtung (VOR) übertragen werden, wo diese in einem Speicher abgelegt werden und auf Anforderung anhand der abgelegten Lizenznachricht (LIZ) überprüft wird, ob der verschlüsselte Teil (VER) des Programms (PRO) zu entschlüsseln ist und abhängig vom Ergebnis dieser Überprüfung der verschlüsselte Teil (VER) mithilfe des abgelegten, digitalen Schlüssels (SCH) entschlüsselt wird.

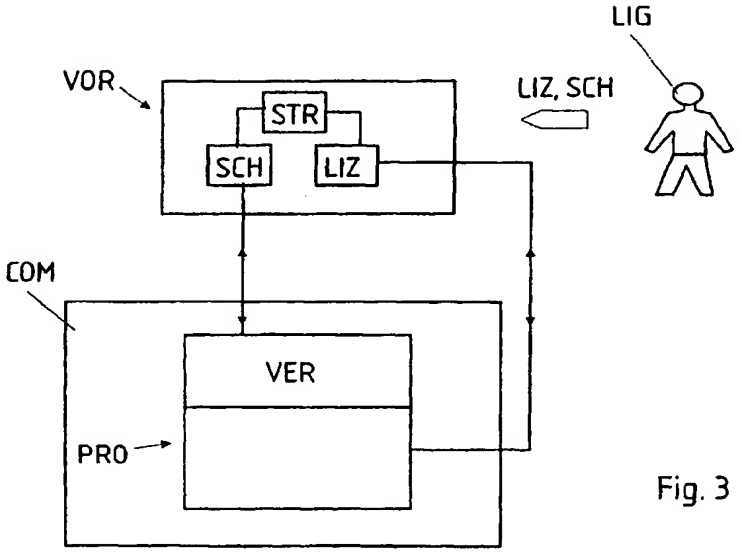

Fig. 3

EP 1 288 768 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 02 45 0147

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
Y	DE 100 01 126 A (INFINEON TECHNOLOGIES AG) 19. Juli 2001 (2001-07-19) * das ganze Dokument *	1,2,10, 12,16, 21,22	G06F1/00
Y	EP 0 989 497 A (CANAL PLUS SA) 29. März 2000 (2000-03-29) * Spalte 7, Zeile 2 - Zeile 38; Abbildung 2 * * Spalte 1, Absatz 1 - Absatz [0003] *	1,2,10, 12,16, 21,22	
E	WO 02 078341 A (THOMSON LICENSING SA ;HORLANDER THOMAS EDWARD (US); HORLANDER KARL) 3. Oktober 2002 (2002-10-03) * Seite 2, Absatz 2 *	2	
Y	EP 1 022 638 A (IBM) 26. Juli 2000 (2000-07-26) * Absatz [0026] *	2	

RECHERCHIERTE SACHGEBIETE (Int.Cl.7)

G06F

~~Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt~~

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	25. Juli 2003	Beker, H.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

Europäisches Patentamt

Nummer der Anmeldung
EP 02 45 0147

GEBÜHRENPFLICHTIGE PATENTANSPRÜCHE

Die vorliegende europäische Patentanmeldung enthielt bei ihrer Einreichung mehr als zehn Patentansprüche.

☐ Nur ein Teil der Anspruchsgebühren wurde innerhalb der vorgeschriebenen Frist entrichtet. Der vorliegende europäische Recherchenbericht wurde für die ersten zehn sowie für jene Patentansprüche erstellt, für die Anspruchsgebühren entrichtet wurden, nämlich Patentansprüche:

☐ Keine der Anspruchsgebühren wurde innerhalb der vorgeschriebenen Frist entrichtet. Der vorliegende europäische Recherchenbericht wurde für die ersten zehn Patentansprüche erstellt.

MANGELNDE EINHEITLICHKEIT DER ERFINDUNG

Nach Auffassung der Recherchenabteilung entspricht die vorliegende europäische Patentanmeldung nicht den Anforderungen an die Einheitlichkeit der Erfindung und enthält mehrere Erfindungen oder Gruppen von Erfindungen, nämlich:

Siehe Ergänzungsblatt B

☐ Alle weiteren Recherchengebühren wurden innerhalb der gesetzten Frist entrichtet. Der vorliegende europäische Recherchenbericht wurde für alle Patentansprüche erstellt.

☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Recherchenabteilung nicht zur Zahlung einer solchen Gebühr aufgefordert.

☐ Nur ein Teil der weiteren Recherchengebühren wurde innerhalb der gesetzten Frist entrichtet. Der vorliegende europäische Recherchenbericht wurde für die Teile der Anmeldung erstellt, die sich auf Erfindungen beziehen, für die Recherchengebühren entrichtet worden sind, nämlich Patentansprüche:

☒ Keine der weiteren Recherchengebühren wurde innerhalb der gesetzten Frist entrichtet. Der vorliegende europäische Recherchenbericht wurde für die Teile der Anmeldung erstellt, die sich auf die zuerst in den Patentansprüchen erwähnte Erfindung beziehen, nämlich Patentansprüche:

1-2,10,12,16,21,22

DOCID: <EP___1288768A3_I_>

Europäisches Patentamt

MANGELNDE EINHEITLICHKEIT DER ERFINDUNG ERGÄNZUNGSBLATT B

Nummer der Anmeldung
EP 02 45 0147

Nach Auffassung der Recherchenabteilung entspricht die vorliegende europäische Patentanmeldung nicht den Anforderungen an die Einheitlichkeit der Erfindung und enthält mehrere Erfindungen oder Gruppen von Erfindungen, nämlich:

1. Ansprüche: 1-2,10,12,16,21,22

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die vorzugsweise in verschlüsselt Form an die genannte Vorrichtung übertragen wird.

   ---

2. Ansprüche: 3,13

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die Zahlungsdaten betreffend die Zahlungsdaten enthält.

   ---

3. Ansprüche: 4,14

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die Zeitdaten betreffend die Gültigkeitsdauer eines Benutzungszeitraumes für das Program enthält.

   ---

4. Ansprüche: 5,15

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, wobei die Vorrichtung anhand einer Signatur die Authenzität eines Programmes überprüft.

   ---

5. Ansprüche: 6,7 ,17,18

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die mittels eines Datennetzes oder Funknetzes übertragen wird.

   ---

6. Ansprüche: 8,19

   Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die über eine Eingabevorrichtung manuell an die Vorrichtung übertragen wird.

Europäisches Patentamt

MANGELNDE EINHEITLICHKEIT DER ERFINDUNG ERGÄNZUNGSBLATT B

Nummer der Anmeldung
EP 02 45 0147

Nach Auffassung der Recherchenabteilung entspricht die vorliegende europäische Patentanmeldung nicht den Anforderungen an die Einheitlichkeit der Erfindung und enthält mehrere Erfindungen oder Gruppen von Erfindungen, nämlich:

---

7. Ansprüche: 11,23

Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, wobei das Program und die Vorrichtung Daten miteinander austauschen.

---

8. Ansprüche: 9,20

Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die Freischaltcodes für noch nicht freigeschaltene Leistungsmerkmale enthält.

---

9. Ansprüche: 9,20

Zugangs/Benutzerkontroller für auf Computern abgelegte Programme unter Verwendung einer mit dem Computer verbindbaren Vorrichtung mit Speicher für Lizenzinformation, die verschlüsselte Teile eines Programms enthält.

DOCID: <EP___1288768A3_I_>

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 02 45 0147

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

25-07-2003

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 10001126 A	19-07-2001	DE 10001126 A1	19-07-2001
		WO 0152017 A1	19-07-2001
EP 0989497 A	29-03-2000	EP 0989497 A1	29-03-2000
		AU 747222 B2	09-05-2002
		AU 9092598 A	12-04-1999
		BR 9812380 A	12-09-2000
		CA 2304148 A1	01-04-1999
		CN 1279784 T	10-01-2001
		EP 1018078 A1	12-07-2000
		HR 20000147 A1	31-12-2000
		HU 0100560 A2	28-06-2001
		WO 9915970 A1	01-04-1999
		JP 2001517833 T	09-10-2001
		NO 20001528 A	25-05-2000
		PL 339457 A1	18-12-2000
		TR 200000779 T2	21-07-2000
		ZA 9808702 A	01-04-1999
WO 02078341 A	03-10-2002	WO 02078341 A2	03-10-2002
EP 1022638 A	26-07-2000	EP 1022638 A2	26-07-2000
		JP 2000206876 A	28-07-2000
		KR 2000057713 A	25-09-2000
		TW 449991 B	11-08-2001

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82